IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, Plaintiff, v. SOLARWINDS CORP. and TIMOTHY G. BROWN, Defendants.	)	Civil Action No. 1:23-cv-09518-PAE-BCM

DECLARATION OF RÓBERT KRAJČÍR IN SUPPORT OF DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

I, Róbert Krajčír, hereby declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, as follows:

1. I make this declaration in support of the motion for summary judgment of Defendants SolarWinds (the "Company") and Timothy Brown (collectively, "Defendants"). The facts set forth herein are based on my personal knowledge. If called upon to do so, I can and will competently testify to these facts.

2. Presently, I am employed by Bohemia Interactive Simulations, a global training and simulation software company, as a Senior Network Engineer. I earned a bachelor's degree in 2012 and a master's degree in 2014, both in computer systems networking and telecommunications, from Brno University of Technology.

3. I worked at SolarWinds as an Intermediate Network Engineer from November 2017 to July 2020, and as a Senior Network Engineer from August 2020 to October 2020. In both roles, I was part of a team responsible for monitoring and supporting portions of SolarWinds' corporate network infrastructure.

4. I have reviewed the representations in SolarWinds' online Security Statement under the heading titled "Role-Based Access Controls." Based on my personal knowledge, those representations were true throughout my time at SolarWinds. The Company provisioned users with access rights based on their role, on a least-privilege-necessary basis, with a formal process to request additional access. For example, when I was onboarded at SolarWinds, I was provisioned with access rights to network systems that I was responsible for managing in my role as a network administrator, which employees outside my team did not have access to. Likewise, there were many systems used by other employees in connection with their roles, which I never had access to.

5. I understand that, in challenging the representations in the Security Statement about role-based access controls, the SEC relies on statements I made in certain emails and a related presentation during my first year at SolarWinds. In those emails and presentation, I raised concerns about the risks of allowing SolarWinds employees or contractors to connect to their SolarWinds accounts remotely, through the Company's virtual private network or "VPN," using their personal laptops, as opposed to laptops issued by SolarWinds. This is a practice sometimes referred to as "Bring Your Own Device" or "BYOD."

6. My concerns about BYOD had nothing to do with role-based access controls or the principle of least privilege. A SolarWinds user using their own personal device to remotely log into their SolarWinds' account would have the same role-based access rights as they would if they logged in to their account using a company-managed device. Those access rights attach to the user's account, not the user's device. My concern regarding BYOD was instead about SolarWinds' ability to monitor user personal devices connected to the network—for example, to monitor whether the devices might be infected with malware. That is a fundamentally different issue from

whether SolarWinds limited users' access rights to those they needed for their jobs. The Security Statement section on role-based access controls does not say anything about the Company's BYOD policies or whether users were required to connect to the Company's network from a company-managed device.

7. I also understand that the SEC has cited language from my emails about what I referred to as "full admin rights" that SolarWinds users had. *See* Ex. A (SW-SEC00666779). The admin rights I was referring to were *local* admin rights that SolarWinds users had on their own SolarWinds-issued laptops—meaning the ability to install software/printers or configure settings *on those laptops*. Those local admin rights are entirely different from *network* admin rights or other sorts of admin rights that would provide access to sensitive data in the Company's databases, systems, and environments. Access to such sensitive data would instead require access rights to the databases, systems, or environments where that data is stored; it would not matter whether the user has local admin rights on their own computer.

8. The reason I mentioned local access rights in the emails at issue is that the solution I was proposing to restrict the VPN to company-issued devices would have required checking devices for company-issued digital certificates before they could log into the VPN. My concern was that, with local admin rights, users could copy these digital certificates from their company-issued devices and port them over to their own personal devices, in order to get around the restriction. Again, this concern had nothing to do with role-based access controls.

[*signature on following page*]

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on: April 24, 2025

Róbert Krajčír